



Information Protection

The Personnel Security Program (PSP) & Supervisors' Responsibilities

Mr. Connolly



Supervisors' Responsibilities Purpose



To provide an overview of supervisors' responsibilities concerning the DoD Personnel Security Program (PSP) as it relates to their employees (civilians, contractors, and military) and employees' access to the network, controlled unclassified information (CUI) and/or classified military information (CMI).



Supervisors' Responsibilities

**DoD Regulations ~~5200.2-R~~ with changes 1,
2, & 3**

**AR 380-67, Personnel Security
AFI 31-501, Personnel Security**

**AR 380-5, Army Information Security
Program
AFI 31-401 - Information Security**

AR 25-2, Information Assurance*

Local Policies & Procedures

***G 6 Regulation, Chap 4 only**



Supervisors' Responsibilities



The success of your security program is based on the principle that security is everyone's responsibility. While each employee is responsible for the protection of national security information, the security supervision of your workforce remains the responsibility of each supervisor. How enthusiastically you assume your security role, and how effectively you use the available resources will have a significant influence on how well you accomplish this responsibility.



Supervisors' Responsibilities



The Personnel Security Program consists of five basic elements:

- 1. Designation of sensitive & public trust positions.**
- 2. Access to classified information/material.**
- 3. Investigation requirements.**
- 4. Adjudication.**
- 5. Continuous Evaluation Program (CEP)**



Supervisors' Responsibilities

1. Designation of Sensitive & Public Trust Positions

Within the DoD, each civilian position is categorized with Respect to security into one of 5 groups:

- **Special Sensitive (SS)**
- **Critical Sensitive (CS)**
- **Non-Critical Sensitive (NCS)**
- **Non-Sensitive (NS)**
- **Public Trust (PT)**



Supervisors' Responsibilities

2. Clearance (access) to Classified Information/Material

This element focuses on access to classified Information or material that has been designated as classified by an original classification authority.

There are 3 levels of classified information:

- TOP SECRET (TS)**
- SECRET (S)**
- CONFIDENTIAL (C)**



Supervisors'

Responsibilities

3. Investigative Requirements

Position Sensitivity	Investigation Type
Special Sensitive (SS) Critical Sensitive (CS) Public Trust (high to moderate risk) (PT)	Single Scope Background Investigation (SSBI)
Non-Critical Sensitive (NCS)	Access National Agency Check with Written Inquiries (ANACI) - Civilians National Agency Check/Local Records Check (NACLC) - Military & Contractors
Non-Sensitive (NS) Public Trust (low risk) (PT)	National Agency Check with Written Inquiries (NACI) - Civilians & Contractors



Supervisors' Responsibilities

4. Adjudication

Adjudication is the evaluation of information contained in an investigation or other documents. A judgment concerning security eligibility is made by evaluating the information

against the DoD Adjudicative

Standards the U.S. Allegiance to the U.S.

- Foreign Influence**
- Foreign Preference**
- Sexual Behavior**
- Personal Conduct**
- Financial Considerations**
- Alcohol Consumption**

- Drug Involvement**
- Psychological Conditions**
- Criminal Conduct**
- Handling Protected Info**
- Outside Activities**
- Use of IT Systems**



Supervisors' Responsibilities

5. Continuous Evaluation Program (CEP)

Once the initial favorable eligibility determination has been made, an individual falls under the Continuous Evaluation Program (CEP).

CEP includes reinvestigation at given intervals based on the types of duties performed and level of access to classified information.

To maintain eligibility, employees must recognize and avoid behaviors that might jeopardize their security clearance or eligibility to perform sensitive duties.

Supervisors are well positioned to remind employees of these responsibilities and encourage reporting when an activity or event may put an employee's



Supervisors' Responsibilities Self-Reporting of Personal Activities

Employees who occupy positions of trust or have access to classified information are expected to self-report changes or incidents that that may impact their access eligibility.

- **Change in personal status**
- **Foreign travel**
- **Foreign contacts**
- **Loss or compromise of information**
- **Financial problems**
- **Arrests**
- **Psychological counseling**



Supervisors'

Responsibilities

Your Responsibilities



esignate civilian positions

review number and access levels - keep to a minimum

new hires - advertise the requirement to obtain and maintain a favorable background investigation

- **Approve access properly (NTK, investigation, NdA)**
- **Keep your Security Manager informed**
- **Emphasize the PSP**
- **Know your people**
- **Provide on-going security training**



Supervisors' Responsibilities Your Responsibilities



Problems in the workplace can often be prevented by timely and appropriate response to warning signs that an individual is under stress or having trouble handling personal problems.

The first step in dealing with any performance problem is normal supervisory counseling. If this does not solve the problem, consider referring the employee to the Employee Assistance Program (EAP). The EAP staff is trained to assess whether or not an employee's performance deficiencies are rooted in some personal problem and, if so, to help the employee deal with these difficulties.



Supervisors' Responsibilities Your Responsibilities



The following warrant referral and possible reporting to the Security Division:

- **Stress**
- **Alcohol problems**
- **Eating disorders**
- **Depression**
- **Sexual addiction**
- **Drug use**
- **Financial problems**
- **Compulsive gambling**



Supervisors' Responsibilities Your Responsibilities



**Start with your activity Security
Manager**

Then...

Roberta Salyer

**Personnel Security Program
Manager**

Roberta.salyer@us.army.mil

757-878-3382



QUESTIONS?

END OF BRIEF



INSTALLATION MANAGEMENT AGENCY



“Sustain, Support and Defend”